Case Study : Data Scrape

LinkedIn

Cyber Attack

Company Description

Company Information:

Industry: Internet
Revenue: $10 billion (2021)
Employee: 18,000 (2022)
Location: United States

- **LinkedIn** is an American business and employment-oriented online service that operates via websites and mobile apps. Launched on May 5, 2003, the platform is primarily used for professional networking and career development and allows job seekers to post their CVs and employers to post jobs. From 2015 most of the company's revenue came from selling access to information about its members to recruiters and sales professionals. Since December 2016, it has been a wholly owned subsidiary of Microsoft. As of February 2022, LinkedIn has 830+ million registered members from over 200 countries and territories.

- The company was founded in December 2002 by Reid Hoffman and the founding team members from PayPal and Socialnet.com (Allen Blue, Eric Ly, Jean-Luc Vaillant, Lee Hower, Konstantin Guericke, Stephen Beitzel, David Eves, Ian McNish, Yan Pujante, Chris Saccheri). In late 2003, Sequoia Capital led the Series A investment in the company. In August 2004, LinkedIn reached 1 million users. In March 2006, LinkedIn achieved its first month of profitability. In April 2007, LinkedIn reached 10 million users. In February 2008, LinkedIn launched a mobile version of the site
- Source: Wikipedia LinkedIn - Wikipedia

Attack Category

The personal information of 92% of LinkedIn users is currently for sale after a data scraping cyber incident..

Description of the Attack :

On June 22, 2021, a hacker announced the sale of over 700,000 pieces of personal information from LinkedIn. In a report detailed by ComputerWeekly.com, almost **all** of LinkedIn's users were impacted by what the organization is calling a data scrape. An investigation into the cyber incident later updated the number to 1 billion records.

Because none of the data was technically stolen, LinkedIn is calling the incident a **Data Scrape**—when an API is used to extract and compile information. Affected users should take measures— like changing their LinkedIn passwords and using extra caution with new connection requests—to prevent their information from being used by cybercriminals.

Risk Assessment Report

Learning Outcome:

Develop a cyber security risk mitigation strategy specific to the organization

1.0 Introduction

1.1 Purpose

- A Risk assessment should be done to determine vulnerabilities within the organization

1.2 Scope of the security risk assessment

- Specify what systems , networks and applications were reviewed as part of the security assessments.
- Determine the role and responsibilities of the team leaders.
- The cost of the security breach and the prevention of further breaches

1.3 Vulnerability sources

- The assessment team will use vulnerabilities sources to help identify potential vulnerabilities

Roles and Responsibilities

NIST Guidelines

Learning outcomes:

Project team should follow the guidelines outlined in the NIST Cybersecurity Framework

www.nist.gov/cyberframework

- Identify- Protect- Detect

- Respond- Recover

Role	Responsibilities
Risk or Project Manager	The Risk Manager identifies risks, verifies if the risk is internal or an external threat.
Integrated Project .Team	This team is responsible for identifying the risks, determining the impact, timing, and priority of the risks.
Risk Owner(s)	The risk owner determines which risks require mitigation and contingency plans. They perform a cost benefit analysis of the proposed strategies. They are also monitoring, controlling and updating the status of the risk.
Other Key Stakeholders	They assist in identifying and determining the context, consequence, impact, timing and priority of the risk.

Vulnerabilities

Impact of the leak data

The data from the leaked files can be used by threat actors against LinkedIn users in multiple ways by:

•Carrying out targeted phishing attacks.

•Spamming 500 million emails and phone numbers.

•Brute-forcing the passwords of LinkedIn profiles and email addresses. The leaked files appear to only contain LinkedIn profile information - we did not find any deeply sensitive data like credit card details or legal documents in the sample posted by the threat actor. With that said, even an email address can be enough for a competent cybercriminal to cause real damage.

Source: Cybernews
LinkedIn Data Breach - 500M Records Leaked and Being Sold | Cybernews
.

Costs & Prevention

Cost

- Following “the dissemination of user data, including IDs, full names, email addresses, telephone numbers” by the threat actor, Italy's privacy watchdog began an investigation into the incident.
- The Italian authority said that the country has one of the highest LinkedIn subscriber counts among European states and called on affected users to “pay particular attention to any anomalies” related to their phone number and their account.

Prevention

- If your LinkedIn profile data might have been scraped by threat actors, we recommend you:
- Use our personal data leak checker to find out if your LinkedIn data has been leaked by the threat actor.
- Beware of suspicious LinkedIn messages and connection requests from strangers.
- Change the password of your LinkedIn and email accounts.
- Consider using a password manager to create strong passwords and store them securely.
- Enable two-factor authentication (2FA) on all your online accounts.

Conclusion

The cyber incident LinkedIn just experienced was a data scrape of users' information and is now up for grabs to the highest bidder. Included in the gleaned data:

What's the difference between a data scrape and a data breach?

In a **data scrape**, data is extracted from publicly available information—as all the information users have on their LinkedIn profile in this case. Data scrapes are not always nefarious in their intent. These data scraping APIs can be used to extract and compile data in large numbers for a valuable purpose.

A **data breach**, on the other hand, is when your confidential information—like your Social Security number, bank or credit card numbers, and email or passwords—are either inadvertently exposed or intentionally stolen by cybercriminals.